



DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2022-OS-0002]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new Department-wide system of records titled, “Defense Mass Transportation Benefits Records (DMTBR),” DoD-0009. This system of records covers DoD’s maintenance of records supporting subsidy programs provided to military and civilian personnel (to include non-appropriated fund (NAF) employees) associated with commuter costs.

DATES: This system of records notice is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic. Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal

identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Privacy and Civil

Liberties Division, Directorate for Privacy, Civil Liberties and FOIA, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700, OSD.DPCLTD@mail.mil, (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing the Defense Mass Transportation Benefits Records (DMTBR), DoD-0009, as a DoD-wide Privacy Act system of records. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

The DoD Mass Transportation Benefit Program encourages employees to use mass transit for commuting to and from work by offering a commuter subsidy as an incentive. The purpose of the program is to reduce traffic congestion and pollution and to improve employee quality of life by providing them commuting flexibility through multiple transportation alternatives. DoD provides mass transportation benefits to offset commuting costs to active duty Service members and civilian personnel (to include NAF employees), as authorized by law and regulation. The program covers a wide variety of alternative transportation modes such as vanpools, commuter trains, and local busses.

DoD SORNs have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Privacy, Civil Liberties, and FOIA Directorate website at <https://dpcl.d.defense.gov>.

II. Privacy Act

Under the Privacy Act, a “system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to OMB and to Congress.

Dated: January 4, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Defense Mass Transportation Benefits Records (DMTBR), DoD-0009.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department’s Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S):

The system manager for records for those who work or are stationed in the Washington, D.C., metropolitan area is the Director, Pentagon Services Division under the Washington Headquarters Services (WHS) Executive Services Directorate at 1155 Defense Pentagon, Washington, DC 20301-1155, whsmc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil. Records concerning those who work or are stationed in other areas of the United States or abroad are maintained by system managers within the Military Departments, Combatant Commands, Defense Agencies, or other Field Activities. To identify the system managers at these components, please visit www.FOIA.gov to contact the relevant component's Freedom of Information Act (FOIA) Office.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 5 U.S.C. 7905, Programs to encourage commuting by means other than single-occupancy motor vehicles; Executive Order (E.O.) 12191, Federal Facility Ridesharing Program; E.O. 13150, Federal Workforce Transportation; DoD Instruction 1000.27, Mass Transportation Benefit Program (MTBP); and E.O. 9397 (SSN).

PURPOSE(S) OF THE SYSTEM:

A. To manage and administer the DoD Mass Transportation Benefit Program for military and civilian personnel (to include non-appropriated fund (NAF) employees) applying for and in receipt of a commuter subsidy.

B. To evaluate employee participation in the program.

C. To provide audit capabilities and track the use of funds to support the program; ensure appropriate accountability; and prevent misuse of the funds involved.

D. To report required information for program management and oversight to leadership and key stakeholders.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Military and civilian personnel (to include NAF employees) applying for and/or receiving a commuter subsidy for using mass transit.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal and Employment information to include: name, Social Security Number (SSN), DoD ID Number, home and work address, email address, official duty telephone number, and organizational affiliation of the individual.

B. Transit information to include: subsidy amount, name of transportation system or company used, benefit provider, point-to-point commuting expenses, commuting distance, locations of travel from initial starting point to destination, number of days an employee commutes per month, type of mass transit used, periodic certifications and reports regarding commuter subsidies, transit authority card numbers, and vanpool owner/operator certifications.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from:

A. Individuals, supervisors, reviewing and approving officials, vanpool owners/operators.

B. Federal, foreign government, State, local and private corporation or business commuter transportation organizations.

C. All DoD databases flowing into or accessed through the following integrated data systems, environments, applications, and tools: WHS Mass Transit Benefits Program, Department of the Navy's Transportation Incentive Program System (TIPS), and the Department of Transportation's TRANServe.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1)

responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

K. To the U.S. Department of Transportation for purposes of verifying DoD military or civilian employees' participation in the program, and auditing and verifying disbursements.

L. To the operators of transit systems or vanpools for purposes of activating, distributing, and verifying benefits.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual's name, SSN, DoD ID number, and/or work email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: DoD components shall retain these records in accordance with National Archives and Records Administration approved General Records Schedule (GRS) 2.4, *Employee Compensation and Benefits Records* (December 2019). These records fall within GRS 2.4, item 131, which provides that transportation subsidy program individual case files may be destroyed two years

after employee participation concludes, but longer retention is authorized if the DoD components have an approved existing agency schedule and have notified the National Archives and Records Administration per 36 CFR 1227a(3).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including CAC authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this

system of records notice along with the full name, current address, and email address of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

CONTESTING RECORD PROCEDURES: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None

HISTORY: None

[FR Doc. 2022-00118 Filed: 1/6/2022 8:45 am; Publication Date: 1/7/2022]